THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	
WRAY, Michael John *et al.*	:	Confirmation No. 8275
U.S. Patent Application No. 10/811,305	:	Group Art Unit: 2131
Filed: March 29, 2004	:	Examiner: Ayaz R. SHEIKH

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: BOARD OF PATENT APPEALS AND INTERFERENCES

BRIEF ON APPEAL

Further to the Notice of Appeal filed February 7, 2008, this Appeal Brief is filed pursuant to 37 CFR § 41.37. The Commissioner is authorized to charge Deposit Account No. 08-2025 in the amount of $510 for the statutory fee.

To the extent necessary, Appellants hereby request any required extension of time under 37 C.F.R. §1.136 and hereby authorizes the Commissioner to charge any required fees not otherwise provided for to Deposit Account No. 08-2025.

TABLE OF CONTENTS

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P., a Texas limited partnership.

II. Related Appeals and Interferences

There are no related appeals and/or interferences.

III. Status of Claims

A. Total Number of Claims in Application

1. There are a total of 12 claims in the application, which are identified as claims 1-12.

B. Status of all the Claims

1. Claims canceled – None
2. Claims withdrawn from consideration but not canceled – None
3. Claims pending – 1-12
4. Claims allowed – None
5. Claims rejected – 1-12

C. Claims on Appeal

1. Claims on appeal are claims 1-12

IV. Status of Amendments

The amendments to the claims, presented in Appellants' Amendment filed September 13, 2007, have been entered.

Entry of the amendments in the after final amendment, filed herewith, is proper under 37 CFR §1.116 since the amendments: (a) do not raise any new issue requiring further search and/or consideration (since the amendments corrects typographical errors); (b) satisfy a requirement of form asserted in the previous Office Action; and (c) place the application in better form for appeal. The amendments are necessary and were not earlier presented because they were unidentified the final rejection.

V. Summary of Claimed Subject Matter

The specification, at paragraphs [0028] – [0041], discloses the trusted computer platform recited in claim 1, wherein at least one security rule relating to at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.

More specifically, the specification, at paragraph [0028] discloses, wherein:

"[0028] [t]rusted computing platform 10, once started, tends to have a compartmented or trusted operating system. This means that one or more services or processes required to be supported by the operating system are run within a compartment which is a logically protected computing environment. As stated above, the actions or privileges within a compartment are constrained (by the security policy), particularly to restrict the ability of a process to execute methods and operations which have an effect outside the compartment, such as methods that request network access or access to files outside of the compartment. In addition, operation of the process within the compartment is performed with a high level of isolation from interference and prying by outside influences."

In addition, at paragraph [0038], the Appellants disclose wherein:

"[0038] [t]he system then switches (at step 121) to a predetermined run-level (which is simply a number 0 - 6, in this case, telling the initialisation process which programs to run). When a service S is started, at step 122, the system obtains a list of the compartments configured for S (at step 124) and ensures that the name of each compartment directory is registered with the kernel as a compartment (the directory called 'default' is ignored at this stage). For each configured compartment C, as determined during step 126, the system starts a rule group called C (step 128), determines whether or not the rule group exists (step 130) and, if so, reads a configuration file to install the configuration variables in the

environment and execute any plugins that are enabled (step 132)." (Emphasis added).

Accordingly, the specification supports Appellants' claim 1 that recites a system comprising a trusted computing platform (10) including:

> at least one first logically protected computing compartment associated with initialization of said system (modules 15), and
>
> at least one second logically protected computing compartment (modules 15), each second logically protected computing compartment being associated with at least one service or process supported by said system,
>
> wherein the system is arranged to load onto said trusted computing platform a predetermined security policy including at least one security rule for controlling the operation of each of said logically protected computing compartments;
>
> wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized (see specification paragraph [0035], steps 114), and wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled (see specification paragraphs [0037] - [0041], steps 132-136).

Regarding claim 12, Figs. 4A and 4B illustrate a flowchart disclosing a method that includes:

> "loading a security policy onto a system including a trusted computing platform (10), said trusted computing platform including at least one first logically protected computing compartments associated with initialization of said system (*see specification paragraphs [0035], [0037] and [0041]*), and at least one second logically protected computing compartments, the

at least one second logically protected computing compartments being associated with at least one service or process supported by said system, said security policy comprising one or more security rules for controlling the operation of said the at least one logically protected computing compartments, the method including the steps of:

loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized (*see specification paragraph [0035], steps 114*), and

loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled (*see specification paragraphs [0037] - [0041], steps 132-136*)."

VI. Grounds of Rejection to be Reviewed on Appeal

The combination of Wiseman et al. (US 7,216,369) in view of Sutton II et al. (US 2003/0229794), does not render claims 1-12 obvious under 35 U.S.C. §103(a).

VII. Argument

Claims 1-12 are patentable under 35 U.S.C. §103(a) over the asserted combination of Wiseman and Sutton for the reasons discussed below. The claims are argued separately and do not stand or fall together.

A. Claim 1

Appellants respectfully submit that the combined disclosures of Wiseman and Sutton do not teach or suggest each and every claim limitation recited in claim 1.

Independent claim 1 recites, *inter alia*, a system comprising a trusted computer platform that includes at least one first logically protected computing compartment, at least one second logically protected computing compartment, and at least one security rule, "wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled." (Emphasis added). In other words, security rules are only loaded when services associated with the rules are enabled. Appellants respectfully submit that the applied art fails to disclose at least this feature of claim 1.

On page 4 of the July 2, 2007 Office Action, the PTO asserts that Wiseman, at column 4, lines 42-55 and 62-67, discloses this feature. Appellants respectfully disagree. At lines column 4, lines 42-55, Wiseman appears to only disclose an alert signal 136 that is generated when a policy is violated, and column 4, lines 62-67, appear only to disclose initialization code 148 that compares the overall configuration and load sequences of the platform at the time of initialization. Nowhere does Wiseman disclose, teach, or suggest, wherein a security code is only loaded "if one or more services or processes are enabled," as recited in claim 1. (Emphasis added). In other words, Appellants recite a system that loads security rules at initialization and when services are enabled, while Wiseman appears to only disclose a system that initiates policies at initialization only.

In the final Office Action, (*see* Response to Arguments section, page 7), the Examiner asserts that "[t]he most reasonable broadest interpretation of this claim includes that no more services or processes are enabled, and therefore initializing only at start up discloses claim 1," (Appellants interpret the Examiner's comment so as mean that initialization is done at startup only). The Examiner then asserts that, based upon this interpretation, Wiseman, at column 3, lines 60-62 discloses the Appellants system. Appellants respectfully disagree.

At the outset, Appellants fail to follow the Examiner's logic. While claim 1 recites a system initialization phase wherein a first logical protected computing

compartment is arranged to be loaded, claim 1 further recites wherein at least one security rule relating to the at least one second logical protected computing compartment is loaded if one or more services or processes associated therewith are enabled. Appellants therefore submit that the Examiner has no support to "reasonable" interpret the claim as loading rules only at startup.

Furthermore, at the cited text, Wiseman appears to only disclose wherein "policy table 118 contains policies to which the platform 102 must adhere during the initialization/boot process." Applicants respectfully submit that neither at this passage, nor at any other passage, does Wiseman disclose wherein services are loaded only when they are enabled, as recited in claim 1.

Sutton appears to only disclose a system for permitting the execution of system management code, and likewise fails to suggest loading a security rule when a service or policy is enabled other than at system initialization.

Based upon the remarks presented above, Applicants respectfully submit that the asserted combination of Wiseman and Sutton present no apparent reason to combine references or modify prior art to create the Applicants' allegedly obvious elements of claim 1.

B. Claim 2

Claim 2 is a system claim according to claim 1, wherein "one or more common variable is defined for each compartment, wherein a relevant security rule is only arranged to be added if the variable associated with a particular compartment is enabled." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

C. Claim 3

Claim 3 is a system claim according to claim 2, wherein "at least one variable associated with a directory of plug-ins is arranged to be added." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

D. Claim 4

Claim 4 is a system claim according to claim 3, wherein "the system is arranged to determine, in response to a compartment being enabled, a status of said at least one variable and cause a relevant plug-in based upon the directory of plug-ins to run only if an associated variable is 'true'." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

E. Claim 5

Claim 5 is a system claim according to claim 4, wherein "the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

F. Claim 6

Claim 6 is a system claim according to claim 5, wherein "the at least one compartment and network resources are arranged so communication between them is provided via relatively narrow kernel level controlled interfaces to a transport

mechanism." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

G. Claim 7

Claim 7 is a system claim according to claim 6, wherein "said communication is governed by rules specified on a compartment by compartment basis." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

H. Claim 8

Claim 8 is a system claim according to claim 7, that includes "means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the at least one security rule associated with that service." Wiseman, at column 5, lines 56-61 appears to only disclose an entry flag indicating the required policy for a section, and fails to disclose means for determining "when" a service is starting. Applicants respectfully submit, therefore, that the asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

I. Claim 9

Claim 9 is a system claim according to claim 8, that includes "means for determining when a service starts, and causing the at least one security rule to be loaded accordingly." Wiseman, at column 5, lines 56-61 appears to only disclose an entry flag indicating the required policy for a section, and fails to disclose means for determining "when" a service is starting. Applicants respectfully submit, therefore, that the asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

J. Claim 10

Claim 10 is a system claim according to claim 1, wherein "the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel." The asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

K. Claim 11

Claim 11 is a system claim according to claim 1, that includes "means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the security rules associated with that service." Wiseman, at column 5, lines 56-61 appears to only disclose an entry flag indicating the required policy for a section, and fails to disclose means for determining "when" a service is starting. Applicants respectfully submit, therefore, that the asserted combination of references present no apparent reason to combine references or modify prior art to create the Applicants' claim elements.

L. Claim 12

Independent claim 12 recites a method of loading a security policy on a system, the method including:

> "loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized, and
>
> loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing

platform only if one or more services or processes associated therewith are enabled." (Emphasis added).

In other words, security rules associated with the second logically protected computing compartments are only loaded when services associated with the rules are enabled. Appellants respectfully submit that the applied art fails to disclose the above listed features of claim 12.

On page 4 of the July 2, 2007 Office Action, the PTO asserts that Wiseman, at column 4, lines 42-55 and 62-67, discloses this feature. Appellants respectfully disagree. At lines column 4, lines 42-55, Wiseman appears to only disclose an alert signal 136 that is generated when a policy is violated, and column 4, lines 62-67, appear only to disclose initialization code 148 that compares the overall configuration and load sequences of the platform at the time of initialization. Nowhere does Wiseman disclose, teach, or suggest, wherein a security code is loaded "only if one or more services or processes associated therewith are enabled," as recited in claim 12.

Furthermore, Sutton appears to only disclose a system for permitting the execution of system management code, and likewise fails to suggest loading a security rule when a service or policy is enabled other than at system initialization.

Based upon the remarks presented above, Applicants respectfully submit that the asserted combination of Wiseman and Sutton present no apparent reason to combine references or modify prior art to create each and every allegedly obvious element of the Applicants' claim 12.

M. Conclusion

Accordingly, Appellant respectfully submits that the rejection of claims 1-12 are in error, and request that the final rejection be reversed.

Respectfully submitted,

Wray *et al.*

Kenneth M. Berner
Registration No. 37,093

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
703-684-1111 Telephone
970-898-0640 Telecopier
Date: March 6, 2008
KMB/ERM/cac

VIII. Claims Appendix

1. A system comprising a trusted computing platform including:

at least one first logically protected computing compartment associated with initialization of said system,

and

at least one second logically protected computing compartment, each second logically protected computing compartment being associated with at least one service or process supported by said system,

wherein the system is arranged to load onto said trusted computing platform a predetermined security policy including at least one security rule for controlling the operation of each of said logically protected computing compartments;

wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized, and

wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.

2. A system according to claim 1, wherein one or more common variable is defined for each compartment, wherein a relevant security rule is only arranged to be added if the variable associated with a particular compartment is enabled.

3. A system according to claim 2, wherein at least one variable associated with a directory of plug-ins is arranged to be added.

4. A system according to claim 3, wherein the system is arranged to determine, in response to a compartment being enabled, a status of said at least one variable and cause a relevant plug-in based upon the directory of plug-ins to run only if an associated variable is 'true'.

5. A system according to claim 4, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.

6. A system according to claim 5, wherein the at least one compartment and network resources are arranged so communication between them is provided via relatively narrow kernel level controlled interfaces to a transport mechanism.

7. A system according to claim 6, wherein said communication is governed by rules specified on a compartment by compartment basis.

8. A system according to claim 7, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the at least one security rule associated with that service.

9. A system according to claim 8, including means for determining when a service starts, and causing the at least one security rule to be loaded accordingly.

10. A system according to claim 1, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.

11. A system according to claim 1, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the security rules associated with that service.

12. A method of loading a security policy onto a system including a trusted computing platform, said trusted computing platform including at least one first logically protected computing compartments associated with initialization of said system, and at least one second logically protected computing compartments, the at least one second logically protected computing compartments being associated with at least one service or process supported by said system, said security policy comprising one or more security rules for controlling the operation of said the at least one logically protected computing compartments, the method including the steps of:

loading said security rules relating to the at least one first logically protected computing compartments onto said trusted computing platform when the system is initialized, and

loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.